DPHHS HAN Info Service Message

Distributed via the DPHHS Health Alert Network (HAN) System

Wednesday, January 25, 2006 1400 hours (2:00 PM MST)

New Information on "Blackworm" e-mail worm virus

As you are probably aware for the last week or so the Security Forums have been buzzing about the latest e-mail worm, known by many names, "Blackworm", being only one of them. It is also known as BlackMal, Nyxem.E, Kama Sutra, W32/MyWife.d, and probably a few others by now.

Those who have state of Montana e-mail will be substantially protected, but other agencies that are not on SummitNet and who do not use State of Montana E-mail should make sure their local anti-virus protection is up-to-date, using the process that local health departments have been required to develop in their previous plans.

The gist of it is that it's a nasty little worm that's payload is designed to overwrite various files on the hard drives of infected machines starting on Feb 3rd and every month on the 3rd after that. The following file types will be overwritten by the virus: DOC, XLS, MDE, MDB, PPT, PPS, RAR, PDF, PSD, DMP, ZIP. The files are overwritten with an error message('DATA Error [47 0F 94 93 F4 K5]').

The State of Montana's Anti-Virus software is able to detect and remove the infected software. Additionally, the State's E-mail Anti-Virus is detecting and killing the virus attachments, so there should be minimal exposure to infection.

However, there is a major hole in many Agencies and Local Governments that will make them vulnerable to this worm. That is Web Based e-mail. Although access to Web Based e-mail is blocked by the web filter, many Agencies and Local Governments have exemptions to this rule. Those with exemptions users of Web Based e-mail have no protection what-so-ever, from the States E-mail Anti-Virus protection, and will be relying totally on their Desktop Anti-Virus for protection from this attack.

In light of this please ensure that your Desktop Anti-Virus protection is current and please make all of your end users that are using Web Based e-mail aware of their exposure in this regard.

There is additional detailed information here: http://isc.sans.org/index.php on this worm.

==

The goal Montana's Health Alert Network is to transmit information to local public health authorities as quickly as possible, and assign a suitable priority to the message that is sensitive to the impact of a health-related event providing information of immediate of utility relative to the public health and safety of Montanans. For questions or comments relative to Montana's HAN system you may contact the Montana State HAN Coordinator Jim Aspevig at <mailto:jaspevig@mt.gov> or the Associate HAN Coordinator Gerry Wheat at <mailto:gwheat@mt.gov>

Categories of Health Alert messages:

Health Alert: conveys the highest level of importance; warrants immediate action or attention.
Health Advisory: provides important information for a specific incident or situation; may not require immediate action.
Health Update: provides updated information regarding an incident or situation; unlikely to require immediate action.
Info Service Message: provides general information regarding a situation or opportunity; does not typically require immediate action.

==